REMARKS

Claims 1-32 and 43-55 are pending in the application.

Claims 1-5, 12-19, and 21-26 are allowed.

Claim 20 is objected to but would be allowable if re-written or amended to overcome the objection set forth in the final Office Action.

Claims 6-11, 27-32, and 43-55 are rejected.

Claims 6, 7, 20, 27, 43, and 49 are amended.

I. Claim Objections

With respect to claim 6, the Office Action objects the claim as informality, and suggests deleting the word "access". Applicant has deleted the word as suggested.

Regarding claim 20, applicant has corrected the typographical error "constants" into "consonants."

II. 35 U.S.C. § 101 Rejections

The Office Action rejects claims 6-11 under 35 U.S.C. § 101 because the disclosed invention is inoperative and therefore lacks utility. The Office Action asserts that "data access" is a process and cannot be encrypted. As discussed above, applicant has deleted the word "access" at line 4 of claim 6 and believes that the objection has been overcome.

III. 35 U.S.C. § 102 Rejections

(a) Jackson

The Office Action rejects claims 6, 27 and 28 under 35 U.S.C. 102 (b) as being anticipated by U.S. Patent 5,793,871 issued to Jackson. (hereinafter "Jackson"). Applicant has amended claims 6 and 27, and believes that the rejection has been overcome.

The Office Action states that Jackson illustrates a method for securing data, comprising the following steps: electrically addressing a spatial light modulator SLM with a stripped data packet from a header stripper (see column 6, lines 18-20 and FIG. 2A, items 204 and 206) to create an image in the 2D pixel array of a spatial light SLM (see col. 6, lines 43-53 and FIG. 2A, items 206); scrambling the readout beam imprinted with the image of the spatial light modulator SLM with a phase scrambling device (see col. 6, lines 27-64 and FIG. 2A, items 206, 207, 209, and 211); and providing the detailed information regarding the original reference beam for decrypting the enciphered data stream (see col. 7, lines 39-60; FIG. 2A, item 215; and FIG. 2B, items "enciphered data packet," 230, 231, 233, 234, and 235).

It appears that the Office Action relies on SLM 206 as the graphical image, thus also as an encryption key. Jackson, however, does not disclose that the graphical image is formed from a character set. Jackson defines the graphical image using the exponential equation (2) at col. 6, line 45. The exponential equation is not a character, a typographical symbol, a set of characters, or a set of typographical symbols. Thus, the graphical image is not formed from a character set or a typographical symbol set.

In light of the above, applicant has amended claim 6 to recite that the graphical image as an encryption key is formed from a character set. Specifically, claim 6 recites the steps of creating a graphical image; encrypting the data using the graphical image as an encryption key, wherein the encryption key is formed from a character set; and providing the capability to utilize said key for gaining access to the data. Applicant believes that the rejection has been overcome.

Similarly, applicant has amended claim 27 to recite that the graphical image is formed from typographical symbols. Thus, Jackson does not anticipate claim 27 as amended. Jackson also does not anticipate claim 28 because claim 28 depends from claim 27.

(b) Cass

The Office Action rejects claims 6-11 and 27-32 under 35 U.S.C. 102 (b) as being anticipated by U.S. Patent 5,946,414 issued to Cass et al. (hereinafter "Cass."). The Office Action states that Cass shows a method for securing data, comprising the following steps: defining signal blocks (see col. 13, lines 50-57 and FIG. 1, item 30); encrypting a message m with the signal blocks (see col. 13, lines 57-67 and FIG. 1, items 200 and 70) so as not to be perceptible to human viewer (see col. 6, lines 56-66); and aligning the signal blocks for recovering message m (see col. 29, lines 15-41 and FIG. 43, items 802, 820, 890, and 898).

It appears that the Office Action relies upon the combination of signal blocks, such as Message Image M in FIG. 4, as the graphical image. Each signal block in Cass includes several smaller regions. See col. 14, lines 12-16. However, the regions are differentiated by color modulations. See col. 14, lines 12-16, and FIG. 2. Thus, the combination of signal blocks, relied upon as the graphical image, is formed from different color modulations, not from a character set or a typographical symbol set.

As discussed above, claim 6 as amended recites that the graphical image as an encryption key is formed from a character set, and claim 27 as amended recites that that the graphical image formed from typographical symbols. Since the combination of signal blocks, which is relied upon as the graphical image, is formed from different color modulations, not from a character set as recited in claims 6 or from typographical symbols as recited in claim 27, Cass does not anticipate these two claims.

Similarly, Cass does not anticipate claims 7-11 for their direct or indirect dependence from claim 6, and does not anticipate claims 29, 31, and 32 for their direct or indirect dependence from claim 27.

Furthermore, claims 7-10, and 29 are not anticipated by Cass for other grounds. Claim 7 recites that the encryption key is formed from a unique set of passwords selected from the character set. Cass discloses that the graphical image is formed from signal blocks. See FIG. 4 as an example. As discussed above, the signal blocks are formed from different color modulations. The two different signal blocks -- one for a binary value of '1' and the other for a binary value of '0' -- are predefined color modulations; they are not passwords selected from the character set. Thus, Cass does not anticipate claim 7 for this reason alone.

Claim 8 recites the steps of generating a randomized MasterGrid as a means for authentication; selecting a particular Master Grid to be associated with the encryption key; and storing the selected MasterGrid for later access as part of the encrypted access to the data. Cass does not disclose a MasterGrid. Even assuming that the combination of signal blocks, such as the one shown in FIG. 4, is considered to be a MasterGrid, the combination is predefined according to the content of the binary input. See FIG. 4. Thus, Cass does not generate a *randomized* MasterGrid, as recited in claim 8. Further, since the MasterGrid is predefined according to the content of the binary input, no selection is needed. Thus, Cass does not anticipate claim 8 for this reason alone.

Claim 9 recites the step of choosing a pathway thru said selected MasterGrid and encoding the chosen pathway as a grid reference. The signal blocks in Cass are arranged in a predetermined manner so that the encoded binary message will always occupy the same positions on a printed page and thereby be properly recognized by the apparatus in which the printed paper is placed to be scanned or read. See col. 13, lines 57-67. Thus, a set of positions is predefined for the encoded binary message, but no pathway is chosen in the predefined set of positions, as recited in claim 9. Thus, Cass does not anticipate claim 9 for this reason alone.

Claim 10 recites that the chosen pathway is encoded as a character string corresponding to the pathway. As discussed earlier, Cass discloses that a binary message is encoded in signal blocks, which are differentiated by different color modulations. See FIGs. 2 and 4. The binary string is encoded not as a character string corresponding to the pathway, as recited in claim 10. Thus, Cass does not anticipate claim 10 for this reason alone.

Claim 29 recites the steps of providing data that is made up typographical symbols; using the graphical image to establish a relationship between the data and other typographical symbols, and replacing the data with the other typographical symbols to mask the data. As discussed above, the Message Image, M, relied upon as the graphical image in Cass, represents the binary data. See FIG. 4. The binary data in Cass is replaced with signal blocks, not other typographical symbols as recited in claim 29. Thus, claim 29 is not anticipated by Cass for this ground alone.

(c) Tomko

The Office Action rejects claims 43-48 and 49-55 under 35 U.S.C. 102 (b) as being anticipated by PCT Publication Number WO 97/05578 by Tomko et al., published February 13, 1997, with a priority date of July 28, 1995 (hereinafter "Tomko").

The Office Action states that Tomko discloses a method and system for accessing an apparatus using a password comprising the following: "an optical beam reflected from a prism surface that is modulated with the characteristics of a fingerprint and then focused onto a camera (see page 6, lines 1-3 and figure 1A, items 12, 14, 16, and 20); encrypting a PIN with finger-print related information (see page 6, lines 3-9 and figure 1A, items 23, 24, 25, and 26); and a device requiring a deciphered PIN decrypted with the fingerprint-related information (see page 6, lines 11-21 and figure 1B, items 16, 204, 208, and 40)."

Tomko seeks to encrypt a PIN using biometric information. See page 2, line 25-page 3, line 5. It then decrypts the PIN using the biometric information. See page 3, lines 5-12. Tomko uses fingerprints as an example for the biometric information. See, for example, FIGs. 1A, 1B, and 2. The Office Action is not clear what item in Tomko constitutes the graphical image in the claims. Since a fingerprint image is the only graphical image in Tomko, the fingerprint image should be interpreted as the graphical image. In encrypting a PIN, Tomko first represents the PIN by a function s(**r**). See Equation (1) on page 6. Tomko then transforms s(**r**) into S(**q**). See Equation (2) on page 7. The fingerprint image is captured by camera 20 and converted to a digital format by an A/D converter 22 to be processed by a processor 24. See FIG. 1A. The fingerprint image is represented by function f(**r**), the Fourier transform of which is F(**q**). See page 7, lines 2-4. Here, **r** and **q** are vectors in 2D spatial and frequency domains, respectively. See page 7, lines 1-4. Tomko then derives an encrypted fingerprint image A(**q**) in the frequency domain from F(**q**) and S(**q**). See Equations (3) and (4) on page 7. Since the fingerprint image f(**r**) is the key for encrypting the PIN, f(**r**) should be interpreted as the graphical image as recited in the claims. The concept of a subset, however, does not apply to a function. Thus, Tomko does not disclose or suggest the concept of a subset of the fingerprint image.

In the decrypting process, the process is just the reverse. See FIG. 1B. Assuming that the input fingerprint image is the same as the one for creating the encrypted finger image A(**q**), S(**q**) can be derived by using F(**q**) and A(**q**) as in Equations (3) and (4). The PIN then can be derived from S(**q**). See Equation (1) on page 6, Equation (2) on page 7, and page 7, line 19-page 8, line 7. In the decrypting process, the fingerprint image in the spatial domain, f(**r**), the fingerprint in the frequency domain, F(**q**), and the encrypted fingerprint image in the frequency domain, A(**q**), have never been displayed.

Furthermore, the Office Action interprets vectors **r** and **q** as lines. At 13. This interpretation is incorrect. Both **r** and **q** are parameters of functions. As known in the art, when a vector is used as a parameter of a function, it is a variable and its components are variables as well. For example, in a 2D domain with x and y as two coordinates, the components of the vector **r** in f(**r**) are pairs of values in the form of (x, y). As used in the art, you can represent f(**r**), as f(x, y). Thus, r and q represent points in the 2D spatial and frequency domains, respectively. Even if these vectors are interpreted as lines, these lines are variables, i.e., the end points of these vectors can be anywhere in the 2D spatial and frequency domains.

Furthermore, since the vectors are just parameters of the image functions not the image functions themselves, whether the parameters form a pattern is irrelevant to the claims such as claim 45.

In light of above, applicant has amended claim 43 to recite the step of displaying the graphical image. Specifically, claim 43 recites the steps of masking the password in a graphical image; displaying the graphical image, and re-constructing the password using the graphical image and input from a user. As discussed above, Tomko does not display the fingerprint image during the decryption process, as recited in claim 43. Thus, Tomko does not anticipate the amended claim 43.

Similarly, Tomko does not anticipate claims 44-48 based on their direct or indirect dependence from claim 43.

Furthermore, claims 44 and 45 are not anticipated by Tomko on different grounds. Claim 44 recites that the graphical image comprises a plurality of cells and the masking step includes selecting a subset of the cells for masking the password. As discussed above, the fingerprint image disclosed in Tomko is represented by a function, f(**r**), in the 2D spatial domain, thus the concept of a subset as recited in claim 44 does not apply.

Claim 45 recites that the selected subset forms a pattern. The Office Action states that "Tomko defines a vector **r** in 2D spatial domain that forms a pattern of a line (see page 7, lines 1-3)." As discussed above, the vector r is only a parameter to image function f(**r**), whether it forms a line is irrelevant because claim 45 recites that the selected subset of the graphical image forms a pattern. Thus, Tomko does not disclose or suggest that the fingerprint image or a subset of it forms a pattern, as recited in claim 45.

Turning to claim 49, the claim as amended recites a secure device for allowing access using a password. The device comprises means for masking the password in a graphical image; means for displaying the graphical image; and means for accepting the re-construction of the password using the graphical image and input from a user. As discussed above the method disclosed in Tomko does not include the step of displaying the graphical image, which should be the fingerprint image shown in FIGs. 1a and 1b. Thus, Tomko does not anticipate claim 49.

Similarly, Tomko does not anticipate claims 50-55 for their direct or indirect dependence from claim 49. Furthermore, Tomko does not anticipate claims 50, 51, and 55 under other grounds. Tomko does not anticipate claims 50 and 51 for the same remarks made above in respect to claims 43 and 45. Turning to claim 55, the claim recites that the accepting means rejects the re-construction if the re-construction does not trace the predetermined sequence. This predetermined sequence refers to the select sequence of a subset of the graphical image as recited in claim 53. As stated in the Office Action, the system disclosed in Tomko will generate an incorrect PIN if the fingerprint used in the decryption is different from that used in the encryption. Tomko, however, does not disclose or suggest tracing a predetermined sequence in a subset of the fingerprint image.

(d) Toyoda

The Office Action rejects claims 43-45, 47, 49-51, 53, and 55 under 35 U.S.C. 102 (b) as being anticipated by U.S. Patent 5,812,278 issued to Toyoda et al. (hereinafter "Toyoda").

The Office Action states that Toyoda illustrates a method and system for accessing an apparatus using a password comprising: "displaying a graphical image (see column 18, lines 35-37 and figure 16); enciphering a pass-word on the basis of the image (see column 18, lines 38-58 and figure 16); and deciphering the pass-word based on the image and determining if the result agrees with a prescribed pass-word (see column 19, lines 24-31 and figure 18, steps S160 and S161)."

Toyoda discloses an image communication method in which an image data communication is performed between an electronic mail apparatus and a facsimile apparatus. One of the problems solved by Toyoda is to prevent unauthorized users from using the facsimile machine. See col. 2, lines 44-50. Toyoda solves the problem by using an enciphered password, which varies with the content of an electronic mail. See col. 19, lines 8-15. An enciphered password is formed by enciphering a password using a cipher key. See col. 18, lines 35-37. The cipher key is obtained from a set of fixed locations in the electronic mail. See FIG. 16, and col. 18, lines 38-41. The password and the cipher key occupy the same number of bytes. See FIG. 16. To form the enciphered password, the password and the cipher key are compared bit-wise. See FIG. 17. If a bit in the password has a value of '1', the corresponding bit in the cipher key is inverted and becomes the corresponding bit in the enciphered password. See FIGs. 16 and 17 and the corresponding description. The receiving facsimile machine deciphers the enciphered password using the same cipher key in the received electronic mail. See FIG. 18. By comparing the deciphered password with a prescribed password, the facsimile machine can verify whether the received electronic mail is authorized. See FIG. 18. In the deciphering process, no user input is necessary.

In light of above, claim 43 is amended to recite that the re-construction step uses input from a user. Specifically, the claim recites the steps of masking the password in a graphical image; displaying the graphical image, and re-constructing the password using the graphical image and input from a user. As discussed above the method disclosed in Toyoda decipher the password using the enciphered password and the cipher key in a received electronic mail. No user input is necessary. Thus, Toyoda does not anticipate claim 43.

Similarly, Toyoda does not anticipate claims 44, 45 and 47 for their dependence from claim 43.

Claim 49 is also amended to recite that the accepting means uses input from a user. Specifically, the claim recites a secure device for allowing access using a password. The device comprises means for masking the password in a graphical image; means for displaying the graphical image; and means for accepting the re-construction of the password using the graphical image and input from a user. As discussed above, Toyoda does not use input from user during the deciphering process. Thus Toyoda does not anticipate claim 49 as well.

Similarly, Toyoda does not anticipate claims 50, 51, 53, and 55 for their dependence from claim 49. Furthermore, Toyoda does not anticipate claim 55 for a different ground. Claim 55 recites that the accepting means rejects the re-construction if the re-construction does not trace the predetermined sequence. This predetermined sequence refers to the select sequence of a subset of the graphical image as recited in claim 53. As stated in the Office Action, the receiver disclosed in Toyoda will transmit error information to the sender if the deciphered password is different from the prescribed password. Toyoda, however, does not disclose or suggest tracing a predetermined sequence in a subset of the electronic mail. In fact, the bit-wise comparison during the deciphering process can be done in any order, for example, from right to left.

IV. Allowed Subject Matter

The Office Action states that claims 1-5, 12-19, and 21-26 are allowed. The Office Action also states that claim 20 would be allowable if rewritten or amended to overcome the objection set forth in this Office Action. Applicant has amended claim 20 and believe that the objection has been overcome. Applicant thanks the Examiner for allowance of these claims.

V. Other Amendments

Claim 7 is amended to indicate that the "character set" has an antecedent. Claim 49 is amended to correct a typographical error.

VI. Summary

Having fully addressed the Examiner's objections and rejections, it is believed that in view of the preceding remarks, this entire application stands in a condition for allowance. If, however, the Examiner is of the opinion that such action cannot be taken, he is invited to contact the applicant's attorney at the number and address below in order that any outstanding issues may be resolved without the necessity of issuing a further Action. An early and favorable response is earnestly solicited.

Please address all future correspondence to Intellectual Property Docket Administrator, Gibbons, Del Deo, Dolan, Griffinger & Vecchione, One Riverfront Plaza, Newark, NJ 07102-5497. Telephone calls should be made to Vincent E. McGeary at (973) 596-4837 or (973) 596-4500.

VII. Fees

If any additional fees are due in respect to this amendment, please also charge them to Deposit Account No. 03-3839.

Respectfully submitted,

Vincent E. McGeary
Attorney for Applicant
Registration No. 42,862

Gibbons, Del Deo, Dolan, Griffinger & Vecchione
One Riverfront Plaza
Newark, NJ 07102-5497

Version With Markings to Show Changes Made

In the Claims:

6. (Twice Amended) A method for securing data and for providing secure access to the data comprising the steps of:

creating a graphical image;

encrypting said data [access] using said graphical image as an encryption key, wherein said encryption key is formed from a character set, and

providing the capability to utilize said key for gaining access to said data.

7. (Amended) The method recited in claim 6 wherein said encryption key is formed from a unique set of passwords selected from [a] the character set, and utilizes a grid forming a matrix of squares.

20. (Amended) The system as recited in claim 12 wherein at least seven of the ten characters are [constants] consonants.

27. (Amended) A method for securing data comprising the steps of:

creating a graphical image; and

masking said data using said graphical image as key, wherein the graphical image is formed from typographical symbols.

43. (Amended) A method for accessing an apparatus using a password

comprising the steps of:

masking said password in a graphical image; [and]

displaying the graphical image; and

re-constructing said password using said graphical image and input from a user.

49. (Amended) A secure device for allowing access using a password, the [apparatus] device comprising:

means for masking said password in a graphical image;

means for displaying said graphical image; and

means for accepting the re-construction of said password using the graphical image and input from a user.